Articles

John Selby/Annelies Moens

Recent Proposals to Reform Data Protection Laws in the EU and Australia

A Comparative Analysis

Data protection laws designed to balance the desire for individual privacy with business and government usage of personal information have spread around the world over the last few decades. After the first wave of regulation in the 1980s and 1990s, the continued growth of internet usage has highlighted shortcomings in those regulations. This has spurred a more recent wave of reform in data protection laws in many jurisdictions. This article gives an overview of recent data protection reform efforts in two federal regulatory systems, the European Union and Australia. It then explores the history of those reform efforts and compares several significant differences between these approaches.

I. Recent Data Protection Reform Efforts in Europe

Whilst several of its member states were early adopters of data protection laws, it was not until 1995 that the European Union adopted a legal framework on data protection at the federal level.[1] Since that time, the growth of the Internet (and, in particular, Internet-based commerce) has created challenges for that legal framework.[2] In 2008, a framework decision created a European Union-wide process for data protection in the context of police cooperation and judicial cooperation in criminal matters.[3] In 2009, the Lisbon Treaty[4] came into effect, which amended the foundational documents for the European Union – the Maastricht Treaty and the Treaty of Rome (renamed as the Treaty on the Functioning of the European Union). Article 16(1) of the latter treaty provides that "everyone has the right to the protection of personal data concerning them" and Article 16(2) grants the European Parliament and the Council authority to create data protection laws.[5]

As a consequence of these developments, in 2010 the European Council adopted its "Stockholm Programme"[6] under which it tasked the European Commission to create a proposal for a new draft Data Protection Regulation (the "proposed regulation").[7] Developed through several rounds of public consultation, conferences, seminars and workshops across the EU member states, the proposed regulation was designed to enhance the internal market of data protection, increase the effectiveness of the fundamental right to data protection, to give individuals control over their data and to enhance the coherence of the EU data protection framework.[8] In 2011, the Commission's proposal was subjected to regulatory impact assessment by the EU's Impact Assessment Board, which required further analysis to be undertaken.[9] Upon presentation of this proposed regulation to the European Parliament, one of its members, Jan Philipp Albrecht (Greens), was appointed as a rapporteur to its Committee on Civil Liberties, Justice and Home Affairs to review that document, seek and collect stakeholder input into it, and propose amendments. On 10 January 2013, Albrecht presented his first draft report to that committee.[10] As several major industries will be affected by the proposed regulation, Albrecht received a heavy volume of comments from industry and NGO stakeholders – two months later his full draft report including stakeholder proposed amendments swelled to 1347 pages.[11]

▷ John Selby, Macquarie University/Annelies Moens, Information Integrity Solutions P/L, both Sydney. This article reflects the personal opinion of the authors and is not an official statement of either employer. Further information about the authors at p. 96.

1 *European Data Protection Directive* 95/46/EC.

2 Three main problem areas were identified by the Commission in its Impact Assessment of the 1995 framework: a) that barriers had emerged for business and public authorities due to fragmentation, legal uncertainty and inconsistent enforcement and administrative burdens; b) difficulties for individuals to stay in control of their personal data; and c) gaps and inconsistencies in the protection of personal data in the field of police and judicial cooperation in criminal matters: European Commission, "Executive Summary of the Impact Assessment" *Commission Staff Working Paper SEC(2012)73*, 2-3.

3 Council Framework 2008/977/JHA of 27 November 2008.

4 "Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community" (2007) 50 *Official Journal of the European Union [http://bookshop.europa.eu/en/official-journal-of-the-european-union-c-306-17.12.2007-pbFXAC07306/downloads/FX-AC-07-306-EN-C/FXAC07306ENC_002.pdf?FileName=FXAC07306ENC_002.pdf&SKU=FXAC07306ENC_PDF&CatalogueNumber=FX-AC-07-306-EN-C]*.

5 "Consolidated Version of the Treaty on the Functioning of the European Union" (2008) 51 *Official Journal of the European Union [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0047:0199:EN:PDF]*.

6 European Council, "The Stockholm Programme – An Open and Secure Europe Serving and Protecting Citizens" (2010) *OJ C 115*.

7 European Commission, "Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation)" 2012/0011 (COD), *[http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf]*.

8 Ibid, 4.

9 Ibid, Explanatory Memorandum, 4-5.

10 Jan Philipp Albrecht, "Draft Report on the Proposal of the European Parliament and of the Council on the Protection of Individual with Regard to the Processing of Personal Data and on the Free Movement of Such Data (COM(2012)0011-C7-0025/2012-2012/0011(COD)) *European Parliament Committee on Civil Liberties, Justice and Home Affairs* 2012/0011.

11 *Monica Horten*, "EU Data Privacy Law Gets a Whopping 3133 Amendments" *IPTegrity* (18 March 2013) *[http://www.iptegrity.com/index.php/european-union/privacy/842-eu-data-privacy-law-gets-a-whopping-3133-amendments]*.

A detailed analysis of the scope of the Commission's proposed regulation is beyond the scope of this article. In summary, when proposing the creation of a single data protection law for the entire European Union, the Commission proposed 91 Articles that sought to:

- ▷ strengthen requirements for consent,
- ▷ increase the accountability of data processors,
- ▷ require public bodies and companies with more than 250 staff to appoint privacy officers,
- ▷ require data holders to notify the regulator and sometimes their customers when data breaches occur,
- ▷ give individuals the rights to be forgotten and to transport their data from one provider to another,
- ▷ impose compliance standards upon non-EU entities if they hold data of EU citizens, and
- ▷ provide for significant penalties for non-compliance (including fines of up to 2 % of worldwide annual turnover for private sector entities and fixed penalties of up to 1 million euros for government entities).

It is also beyond the scope of this article to go into specific details on the many amendments proposed by Rapporteur Albrecht and industry stakeholders in his draft report. In summary, Albrecht proposed to:

- ▷ broaden the definition of personal data,
- ▷ include stronger consent rules (opt-in rather than opt-out),
- ▷ expand the right to access information to include the ability to obtain information about profiling and whether other agencies had requested data, and
- ▷ require greater privacy awareness through multi-layered notifications and standardized coloured privacy icons.

As of mid-May 2013, the European Parliament's vote on the Proposed Regulation originally planned for 29 May has been delayed as the Committee requires additional time to consider the heavy volume of proposed amendments.[12] As the Irish President of the EU has supported this initiative, a vote is likely (though not certain) to occur before the rotation of the Presidency on 1 July.[13]

Having given an overview of recent data protection regulatory reform efforts in the European Union, the next section gives an overview of recent reform efforts in Australia.

II. Recent Data Protection Reform Efforts in Australia

Unlike the European Union where several member states passed specific data protection legislation prior to the creation of a federal framework, in Australia specific data protection law was first passed at the federal level, with some state laws enacted thereafter.[14] The federal government passed its Privacy Act in 1988, which created privacy principles for government agencies (Information Privacy Principles).[15] In 2001, amendments came into effect to expand coverage to private sector entities with a different set of privacy principles (National Privacy Principles).[16] For the next decade, the Privacy Act (Cth) was not the subject of significant amendments until 2012. The remainder of this section explores how and why these recent amendments occurred. The next section explores the key changes introduced by those amendments.

1. Move Towards Accountability – Rather Than the EU Model of Adequacy

The *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) ("amended Privacy Act") passed by the Australian Parliament on 29 November 2012 and assented to on 12 December 2012 will make significant changes to the existing Australian Privacy Act.[17]

a) Stage One

It has taken six years from the commencement of the Australian Law Reform Commission's Review (ALRC) of the Privacy Act to the passage in 2012 of the first round of amendments to the Privacy Act.[18] Further amendments are proposed, as the 2012 amendments only reflected the first of two stages due to the volume of recommendations made by the ALRC.[19] The ALRC spent 28 months reviewing the Privacy Act and made 295 recommendations. Its report was released on 12 August 2008 and entitled *"For Your Information: Australian Privacy Law and Practice"* (ALRC Report 108).

The Australian government decided to respond to the ALRC Report in two stages, with the first stage now complete as evidenced by the passage of the amended Privacy Act.[20] However, it is expected that the Attorney-General will conduct a review of the operation of certain aspects of the amended Privacy Act, one year after it commences based on the Report of the House of Representatives Standing Committee on Social Policy and Legal Affairs' Inquiry to the Bill prior to passage.[21]

12 This includes comments from lobbyists and even by the Office of the President of the Council of Europe, a copy of which leaked at: *[http://www.statewatch.org/news/2013/may/eu-coe-data-protection-8825-13.pdf]*.

13 PC World, "EU Data Protection Vote Delayed Again" *[http://www.pcworld.com/article/2038072/eu-data-protection-vote-delayed-again.html]*; *Cecile Park*, "EU: Three Possible Dates Put Forward for the LIBE Vote on Data Protection" *[http://dataguidance.com/news.asp?id=2020]*.

14 The Privacy Act (Cth) 1988 pre-dates legislation passed in New South Wales (1998), Australian Capital Territory (1988), Victoria (2000), Northern Territory (2002), Tasmania (2004) and Queensland (2009). The state governments of Western Australia and South Australia have not yet passed specific privacy legislation. For more information, see: Office of the Federal Privacy Commissioner, *Links [http://www.privacy.gov.au/links#2]*.

15 Privacy Act (Cth) 1988 *[http://www.austlii.edu.au/au/legis/cth/num_act/pa1988108/]*.

16 Privacy Amendment (Private Sector) Act (Cth) 2000 *[http://www.austlii.edu.au/au/legis/cth/num_act/pasa2000346/]*.

17 The amendments become operational on 12 March 2014, 15 months after the Amendment Act received Royal Assent. This period of time enables entities bound the Act to adapt to the changes, as there are no transitional provisions in the legislation.

18 Australian Law Reform Commission, "For Your Information: Australian Privacy Law and Practice" (2008) *Volumes 1–3 [http://www.alrc.gov.au/publications/report-108]*.

19 Department of Prime Minister & Cabinet, "Enhancing National Privacy Protection, Australian Government First Stage Response to the ALRC Report 108 For Your Information: Australian Privacy Law and Practice *[http://www.dpmc.gov.au/privacy/alrc_docs/stage1_aus_govt_response.pdf]*.

20 Ibid.

21 House of Representatives Standing Committee on Social Policy and Legal Affairs, "Advisory Report: Privacy Amendment (Enhancing Privacy Protection) Bill" (2012), p11. *[http://www.aph.gov.au/Parliament*

The stage one amendments create a new unified set of privacy principles for both private and public sectors, called the Australian Privacy Principles (APPs), introduce comprehensive credit reporting requirements, and increased powers for the Commissioner.

b) Stage Two

The remaining issues that remain to be addressed and which form stage two include whether or not mandatory data breach notification should be introduced, whether the small business, employee exemption and other exemptions should be removed and whether a statutory tort for invasion of privacy should be introduced.[22] The latter has recently been referred back to the ALRC, which in its ALRC Report 108 had suggested this should be introduced.[23]

Very recently, a copy of the Government's latest draft Bill which would further amend the Privacy Act was leaked to industry journalists.[24] This draft Bill includes provisions which would require mandatory notification by both public sector and private sector entities bound by the Act of the occurrence of "serious data breaches". Disclosure would have to be made to the Privacy Commissioner, to the general public via the entity's website/a major public newspaper, and (in some circumstances) to the affected individuals.[25]

2. Key Changes – Amendment Act

The Amended Privacy Act makes significant changes in three main areas: (a) it increases the powers of the Australian Privacy Commissioner; (b) it unifies the existing Information Privacy Principles and National Privacy Principles into a combined Australian Privacy Principles; and (c) it creates a comprehensive credit reporting regime. Each of these three changes is discussed below.

a) Increased Powers for the Commissioner

Under the amended Privacy Act, the Commissioner wields increased powers, particularly relating to referral to Court for breaches of provisions subject to civil penalties, the conduct of own motion investigations with teeth and the ability to conduct assessments (audit type of powers) of entities subject to the Act and require government agencies to conduct privacy impact assessments.

aa) Complaints

When investigating complaints lodged by individuals whose privacy has allegedly been interfered with, the Commissioner under the amended Privacy Act will have the ability to apply to the Federal Court or Federal Magistrates Court for an order that an entity alleged to have contravened a civil penalty provision pay the Commonwealth a pecuniary penalty.[26] This can occur in situations where there have been serious and repeated interferences with privacy or credit reporting provisions have been breached.[27]

As discussed in 7) below, civil penalty orders for body corporates can reach $1.7 million and for individuals $340,000 (or potentially even higher depending upon how the courts interpret breaches of this section).[28] The Federal Court or Federal Magistrates Court may also make compensation orders for individuals that have suffered as result of the breach. The Commissioner may also accept undertakings that are enforceable by the Federal Court or Federal Magistrates Court[29].

bb) Own Motion Investigations

The Commissioner has a power to conduct "own motion investigations" in circumstances where a complaint is not lodged, but the Commissioner is of the view that due to the nature of information brought to his attention, through media or some other source, an investigation is warranted.[30]

Traditionally, own motion investigations have represented a very small percentage of all investigations.[31] Until the Amending Act comes into effect, the Commissioner has no powers to impose sanctions as a result of an own motion investigation. Whilst the Commissioner could make recommendations and suggestions to the investigated entity, if that entity chose not to act on those recommendations the Commissioner has no enforcement power other than to simply publish findings. The new amendments now provide the Commissioner with the same powers as if they were investigating a complaint made by an individual as outlined above.[32]

This is significant as large scale systemic issues are usually the subject of own motion investigations, as such the Commissioner dedicates resources here due to pervasive privacy issues that appear to arise affecting the privacy of a number of individuals.

cc) Assessments

The Commissioner now has increased audit powers, in that they may make assessments as they see fit of entities bound by the Act to determine whether or not they are in compliance with the privacy principles and/or credit reporting provisions.[33] The Commissioner may also order government agencies bound by the Act to conduct a Privacy Impact Assessment if an activity or function of the agency has a significant impact on the privacy of individuals.[34]

b) New Australian Privacy Principles

The Amended Privacy Act removes the Information Privacy Principles that applied to Federal and ACT govern-

ary_Business/Committees/House_of_Representatives_Committees?url=spla/bill%20privacy/report.htm].

22 Department of Prime Minister & Cabinet, above n19, p14.

23 *Chris Merritt*, "Labor shelves privacy tort plan", *The Australian* (13 March 2013), *[http://www.theaustralian.com.au/media/labor-shelves-privacy-tort-plan/story-e6frg996-1226595931407].*

24 Darren Pauli, "Exposed: Australia's Data Breach Laws" *IT NEWS* (2 May 2013) *[http://www.itnews.com.au/News/341779,exposed-australias-data-breach-laws.aspx];* Secure Computing, "Mandatory Data Breach Notification: A Guide to Compliance" *Summary of Leaked Draft Bill [http://i.haymarket.net.au/Assets/Breach20Compliance20Guide.pdf].*

25 Ibid.

26 Privacy Act, section 80U.

27 Ibid, section 13G.

28 The *Crimes Act 1914* (Cth) outlines the value of a penalty unit and in January 2013 increased the value of penalty units (s4AA).

29 Privacy Act, above n26, section 33E.

30 Ibid, section 40(2).

31 Between 1 July 2011 and 30 June 2012, the Commissioner commenced 37 own motion investigations, as opposed to receiving 1,357 complaints: 2011-2012 OAIC Annual Report *[http://www.oaic.gov.au/publications/reports/annual-report_11-12/chapter6.html#p3].*

32 Privacy Act, above n26, section 52(1A).

33 Ibid, Section 33C.

34 Ibid, Section 33D.

ment agencies and the separate National Privacy Principles that applied to the private sector.[35] It effectively merges, with a few changes, these two separate sets of principles into one set of Australian Privacy Principles applicable to both public and private sector entities that need to comply with privacy legislation.

Outlined below are the significant substantive changes to these privacy principles:

aa) APP 1 and 5

APP 1 calls for a clear and renewed focus on open and transparent management of personal information. It has an overt requirement to demonstrate that steps – such as practices, procedures and systems are in place to comply with the APPs and handle complaints that may arise. This provision also sets out the requirements for what needs to be contained within privacy policies, including if personal information is likely to be disclosed offshore and the list of those countries. This also applies at the point of collecting personal information from individuals as outlined in APP 5.[36]

bb) APP 4

This is a new principle governing the collection of unsolicited personal information. If the APP entity determines the information is personal information it would not normally collect for its functions or activities in accordance with APP 3, then the personal information needs to be destroyed or de-identified, subject to some minor exceptions relating to Commonwealth records.[37]

cc) APP 7

This principle states that an entity must not use or disclose personal information for the purpose of direct marketing and then proceeds to provide exceptions to allow this to occur. These include where the individual consents and prominent opt-out facilities are provided in direct marketing communications. Individuals also have the right to find out the source from where the organisation obtained their personal information. This is a new right. In practice, this is a common concern for individuals who receive direct marketing, particularly when they have had no prior relationship with the entity sending them direct marketing communications.[38]

dd) APP 8

This principle replaces the cross border privacy principle found in National Privacy Principle (NPP) 9. The new principle is designed on the basis of "accountability" found within APEC privacy principles, as opposed to "adequacy" found in the EU privacy principles. There are 21 member economies in APEC, including Australia and the United States and many Asian countries.[39]

APP 8 is also different to NPP 9 in that it relates to disclosure of personal information offshore, rather than transfer. This in effect means that the offshore recipient entity does not need to hold the record for this principle to become relevant.

APP 8.1 needs to be read in conjunction with section 16C of the amended Privacy Act. It holds the Australian APP entity accountable for actions/inactions of the overseas recipient should they do an act which the Commissioner would consider to be a breach. There are some exceptions to the accountability provision in APP 8.1, which are enumerated in APP 8.2.

The two key exceptions set out in APP 8.2 relate to having 1) obtained consent from the individual for the offshore disclosure or 2) disclosing personal information to a recipient based in a country with substantially similar privacy law to the Australian privacy principles which can be enforced or the recipient is a subject to an enforceable binding scheme.[40]

It is important to note here that many offshore entities to which Australian companies disclose personal information are located in APEC member economies. In the last two-three years many Asian data protection laws have been amended or, in the cases of Singapore, Philippines and Malaysia, been introduced for the first time.[41] There is no approved official list of countries that may be considered to have substantially similar privacy law to the Australian privacy principles. There is perhaps more scope for use of binding schemes, such as the relatively new Cross-Border Privacy Rules developed within the APEC Privacy Framework for member economies.[42] This regime is akin to the Binding Corporate Rules (BCR) process in the EU, but is less likely to suffer from the same delays that are experienced with the BCR process.[43]

c) Comprehensive Credit Reporting Regime

The amended Privacy Act introduces a comprehensive credit reporting regime, whereby rather than just collecting and disclosing "negative" credit information in legally allowed circumstances under the Privacy Act, there is now the possibility of including "positive" information, such as open account information.[44] This brings Australia in line with most other countries around the world which already have comprehensive credit reporting regimes.

The changes here include allowing, subject to improved privacy protections, the reporting of five new kinds of personal information:

- the date the consumer credit account was opened
- the type of consumer credit account opened
- the date the consumer credit account was closed
- the maximum amount of credit available under the consumer credit account and

35 Privacy Amendment (Enhancing Privacy Protection) Act 2012 *[http://www.comlaw.gov.au/Details/C2012A00197]*.
36 Ibid, Schedule 1.
37 Ibid.
38 Ibid.
39 APEC Member Economies *[http://www.apec.org/about-us/about-apec/member-economies.aspx]*.
40 Schedule 1, Privacy Amendment (Enhancing Privacy Protection) Act 2012 *[http://www.comlaw.gov.au/Details/C2012A00197]*.
41 Singapore, Personal Data Protection Act 2012; Philippines, Data Privacy Act 2012; Malaysia, Personal Data Protection Act 2010.
42 APEC, "Cross-Border Privacy Rules System Goes Public", 31 July 2012 *[http://www.apec.org/press/news-releases/2012/0731_cbpr.aspx]*.
43 UK Information Commissioner's Office, "Binding Corporate Rules" *[http://ico.org.uk/for_organisations/data_protection/overseas/binding_corporate_rules]*.
44 Schedule 2, Privacy Amendment (Enhancing Privacy Protection) Act 2012 *[http://www.comlaw.gov.au/Details/C2012A00197]*.

- repayment performance history about a person over the last two years and the number of repayment cycles that person was in arrears.[45]

The above new kinds of personal information can be retained on a consumer credit information file for up to two years only. This contrasts with default information which can be retained on a consumer credit information file for up to 5 years.[46]

Individuals have the new right to request that their personal information not be used or disclosed by a credit reporting body if they reasonably suspect identify theft or fraud.[47] Credit reporting bodies and credit providers must have clear and up-to-date information policies.[48] A new credit reporting code will also still need to be approved by the Commissioner which will manage many of the day-to-day operations of the credit reporting system.[49] The new powers as outlined under "Increased Powers for the Commissioner" apply to the credit reporting provisions as well.[50]

III. Significant Differences between European and Australian Approach

Whilst there are a great many more specific differences which could be discussed, this article focuses upon seven aspects of the differences between the approaches in the European Union and Australia resulting from these recent proposed amendments to Data Protection Laws. In particular, it considers the desire for consistency across state borders, the expanded recognition of individual rights to privacy, the definition of personal data, consent, notification, the appointment of data protection officers and penalties are discussed below.

1. Consistency Across State Borders

One of the stated goals of the proposed regulation in the EU is to overcome the failure of the directive to "achieve a proper harmonization due to the different implementation of its provisions by member states".[51]The amendments to the Privacy Act at the Commonwealth level in Australia do not seek to compel the governments in each of the Australian states to pass/amend their existing data protection legislation to operate in a manner consistent with the federal Privacy Act. State-based legislation will continue to provide inconsistent data protection rights and protections for residents of each state when dealing with their state government agencies. However, when dealing with federal government agencies or the private sector, consistent data protection laws will operate under the federal law.

2. Expanded Recognition of Individual Rights to Privacy

The EU proposes to expand individual rights to privacy through a right to be forgotten and a right to data portability.[52] Neither of these rights has yet been proposed in Australia – by either the Australian Law Reform Commission or the Australian government. Although Australia does not have an American-style Bill of Rights or an EU-style Charter of Fundamental Rights[53], it is possible (though not a certainty) that if the EU recognises these expanded data protection rights, the Australian Parliament may (in the medium- to long-term) incorporate similar rights into future amendments to the Privacy Act.

3. Definition of Personal Data

The latest EU proposal would expand the definition of personal data to include pseudonymous data and objective criteria.[54] Neither of these feature in existing or proposed changes to Australian data protection law.

4. Consent

The Albrecht Report included proposals for standardised logos and icons to assist individuals to more easily assess whether to grant consent to the collection, use and disclosure of their personal information.[55] Neither of these feature in existing or proposed changes to Australian data protection law.

5. Notification

The Albrecht Report proposed to extend the time frame within which personal data breaches had to be notified to the regulator from 24 hours to 72 hours, and to reduce the number of breaches reported by requiring notification only for breaches likely to affect adversely the protection of personal data or the privacy of the data subject.[56] The leaked draft data breach notification Bill in Australia to amend the Privacy Act did not include specific time limits, requiring instead notification "as soon as practicable" after an entity has formed a belief on reasonable grounds that such a serious breach has occurred.[57]

6. Appointment of Data Protection Officers

The Albrecht Report proposes that the obligation on private sector entities to appoint Data Protection Officers should be on the basis of the volume of personal data processed by that entity rather than on the entity's turnover or number of employees.[58] Existing and proposed Australian data protection laws do not include requirements for the appointment of data protection officers.

7. Penalties

The Albrecht Report reiterates the Draft Regulation's proposal that the maximum fine for a privacy breach be 1 million Euros or, in the case of an enterprise, two percent of its annual worldwide turnover.[59] In Australia, the proposed maximum fine for a privacy breach is

45 Privacy Act, above n26, section 6N.
46 Ibid, section 20W.
47 Ibid, section 20K.
48 Ibid, sections 20B and 21B.
49 Ibid, Part IIIAA.
50 Ibid, Part IIIA.
51 Explanatory Statement to the Albrecht Draft Report dated 17 December 2012, p209.
52 Ibid, p212; Proposed Articles 15(2a) and 17.
53 European Union, Charter of Fundamental Rights of the European Union, (2000/C 364/01) *[http://www.europarl.europa.eu/charter/pdf/text_en.pdf]*.
54 Albrecht Report, p211; Proposed Articles 4(1) and 4(2)(a).
55 Ibid, p211; Proposed Articles 11(2a) and 11(2b).
56 Ibid, p213; Proposed Articles 31 and 32.
57 Secure Computing, above n25.
58 Ibid, p212; Proposed Articles 14 and 28.
59 Ibid, p190; Proposed Article 79.

$A1.7 million (approximately 1.33 million Euros at May 2013 exchange rates), though it is unclear as to whether such a fine would be imposed by a court on a per breach basis, or per individual who has suffered from that breach.[60]

8. Adequacy vs Accountability

Unlike Article 25 of the 1995 Data Protection Directive which permits transfers by data controller of data to countries outside the EU if those countries have adequate data protection laws, the concept of discloser accountability under the new APP 8 in Australia focuses upon the ability of the recipient to protect the information rather than whether the laws of the recipient's country provide adequate protection for that personal information. This accountability concept was developed as APEC Principle 26 and permits data transfers to compliant recipients in non-compliant countries whilst preventing such transfers to non-compliant recipients even if that recipient operates in a country which might otherwise be regarded as having adequate data protection laws.

60 See discussion above near n26.

IV. Conclusion

Both the European Union and Australia are in the midst of their respective processes through which they will update their data protection laws to keep pace with technological change. Whilst there are some similarities between their proposed laws, there are also differences. Arguably, the APEC Privacy Framework with its focus on accountability has had greater impact in Australia whilst having little to no impact on the EU. The Australian data protection reforms are not as ambitious as those proposed in the EU. In particular, proposals which would see expansions to the privacy rights of individuals, a widened definition of personal data, simplified consent iconography, more stringent breach notification requirements and compulsory appointment of data protection officers in the EU are not being proposed in Australia. If these proposals are implemented in the EU, Australia would risk falling further into "inadequate" compliance status for cross-border data transfer requirements. However, it is possible that the APEC Cross-Border Privacy Rules may play an increasingly significant role in the future in enabling Australian-based entities to conduct business with EU citizens.[61]

61 APEC Committee on Trade and Investment, "APEC Cross-Border Privacy System Rules", *[http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx]*.